					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: PII24					Documenttitel: **Privacybeleid voor CCTV en fysieke monitoring**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/beheersmaatregel/artikel	Toepasselijkheid	Dekkingstype	Opmerking
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Gedocumenteerde en operationele beheersmaatregelen
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring en corrigerende maatregelen
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Doel, rechtsgrondslag, risicotrigger en registraties
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Toewijzing aan verwerker en gezamenlijke verwerkingsverantwoordelijke
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10	Controller	Supporting	Verplichtingen en verzoeken van betrokkenen
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Verzameling, verwerking, minimalisatie, bewaring en verwijdering
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Registraties en verzoeken inzake verstrekking
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Verwerkersovereenkomsten, instructies, ondersteuning en registraties
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Rechten van verwerkers en ondersteuning bij verstrekking
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Bescherming van registraties en logging
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Beginselen en verantwoordingsplicht
GDPR	Article 6	Controller	Primary	Rechtsgrondslag
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparantie en privacyverklaringen
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Verzoeken tot uitoefening van rechten

GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Governance, verwerkers, registraties, beveiliging, DPIA en advies
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Doel, verzameling, minimalisatie, bewaring en verstrekking
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparantie, participatie, verantwoordingsplicht, beveiliging en naleving
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Privacyrisico en DPIA-triggers
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Privacybeheersmaatregelen voor bescherming van PII
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Beheersmaatregelen voor toegang en fysieke toegang
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, fysieke monitoring, toegangsbeperking en logging

1. Reikwijdte

1.1 Dit beleid is van toepassing op CCTV, videomonitoring, bezoekersmonitoring, fysieke toegangscontrolelogboeken, door beveiligingspersoneel uitgevoerde monitoringregistraties, systemen voor monitoring van locaties en daarmee samenhangende fysieke monitoringactiviteiten waarbij PII wordt verzameld of anderszins verwerkt.

1.2 Dit beleid is van toepassing op organisaties die optreden als PII-verwerkingsverantwoordelijke voor hun eigen locaties en fysieke monitoringactiviteiten.

1.3 Het is ook van toepassing op ondersteunende activiteiten als verwerker of subverwerker wanneer de organisatie camerabeelden, bezoekersgegevens of fysieke toegangslogboeken namens een klant beheert, host, beoordeelt, opslaat, verstrekt, verwijdert of anderszins verwerkt.

1.4 Dit beleid omvat de vaststelling van monitoringdoelen, goedkeuring, privacyverklaringen en bebording, toegangsbeperkingen, verstrekking, bewaring, verwijdering, uitbesteding, escalatie van incidenten, routing van verzoeken tot uitoefening van rechten, beoordeling en beheer van bewijsmateriaal.

1.5 Dit beleid bevat geen arbeidsrechtelijk advies, juridische toelichting over ondernemingsraden, procedures voor opsporingsinstanties of een afzonderlijk CCTV-register.

1.6 Monitoringspecifiek bewijsmateriaal wordt bijgehouden in de canonieke PIMS-bewijsobjecten die in dit beleid zijn genoemd.

2. Doel

2.1 Het doel van dit beleid is privacybeheersmaatregelen voor CCTV en fysieke monitoring vast te stellen, zodat monitoringactiviteiten doelgericht, transparant, proportioneel en toegangsbeheerst zijn, gedurende vastgestelde perioden worden bewaard, uitsluitend via goedgekeurde kanalen worden verstrekt en worden ondersteund door auditeerbaar PIMS-bewijsmateriaal.

2.2 Dit beleid ondersteunt een consistente behandeling van camerabeelden, bezoekersregistraties, fysieke toegangslogboeken en daarmee samenhangende PII uit monitoring, zonder aanvullende registers, comités, dashboards of niet-canonieke rollen te creëren.

3. Doelstellingen

3.1 De doelstellingen van dit beleid zijn om:

3.1.1 monitoringdoelen en de reikwijdte van de verwerking vast te stellen voordat monitoring begint;

3.1.2 CCTV-, fysieke toegangs-, bezoekersmonitoring- en fysieke monitoringactiviteiten in REG02 te documenteren;

3.1.3 monitoringactiviteiten te identificeren waarvoor een beoordeling van privacyrisico's of DPIA-screening in REG04 vereist is;

3.1.4 transparant bewijsmateriaal voor privacyverklaringen en bebording in REG07 bij te houden;

3.1.5 toegang tot, bekijken, export, verstrekking en bewaring van PII uit monitoring te beperken;

3.1.6 verzoeken van betrokkenen via REG06 te routeren;

3.1.7 uitbestede monitoringaanbieders en bewijsmateriaal voor gegevensdeling via REG08 te beheren;

3.1.8 vermoedelijke PII-incidenten in verband met monitoring via REG10 te escaleren;

3.1.9 beoordelingen, uitzonderingen, non-conformiteiten, corrigerende maatregelen, auditbevindingen en verbeteringen in REG12 vast te leggen.

4. Beleidsverklaringen

4.1 Monitoringinventaris, doel en goedkeuring

4.1.1 [Controller] De Process Owner / Business Owner MOET elke CCTV-activiteit, bezoekersmonitoringactiviteit, fysieke toegangscontrolelogboekactiviteit of fysieke monitoringactiviteit in REG02 registreren voordat de activiteit begint.

4.1.2 [Controller] De Privacy Lead / PIMS Manager MOET de REG02-registratie valideren op doel, rechtsgrondslag, gemonitorde locatie, PII-categorieën, categorieën betrokkenen, bewaring, privacyverklaring, toegang en verstrekkingsvelden voordat een nieuwe of wezenlijk gewijzigde monitoringactiviteit wordt geactiveerd.

4.1.3 [Controller] De Process Owner / Business Owner MOET goedgekeurde gemonitorde zones, uitgesloten zones en verzamelingsgrenzen in REG02 registreren voordat camera's, sensoren, bezoekerslogboeken of logging van toegangscontrole worden ingeschakeld.

4.1.4 [Conditional] De Process Owner / Business Owner MOET een privacyrisicobesluit in REG04 verkrijgen voordat monitoring wordt geactiveerd waarbij sprake is van systematische monitoring, audio-opname, biometrische identificatie, detectie met analytics, gevoelige locaties, kwetsbare personen of niet-zichtbare monitoring.

4.1.5 [Joint Controller] De Privacy Lead / PIMS Manager MOET de verdeling van gezamenlijke monitoringverantwoordelijkheden in REG08 vastleggen voordat gedeelde monitoring met een verhuurder, facilitaire partner, klant of andere gezamenlijke verwerkingsverantwoordelijke begint.

4.1.6 [Processor] De Privacy Lead / PIMS Manager MOET klantinstructies voor monitoring en toegestane verwerkingsgrenzen in REG08 vastleggen voordat camerabeelden, bezoekersregistraties of fysieke toegangslogboeken namens een klant worden verwerkt.

4.2 Privacyverklaring en transparantie

4.2.1 [Controller] De Process Owner / Business Owner MOET ervoor zorgen dat bewijsmateriaal voor monitoringbebording of een gelijkwaardige just-in-time privacyverklaring in REG07 wordt vastgelegd voordat gemonitorde gebieden voor betrokkenen worden geopend.

4.2.2 [Controller] De Privacy Lead / PIMS Manager MOET elke monitoringprivacyverklaring in REG07 koppelen aan het bijbehorende verwerkingsdoel in REG02 vóór publicatie of een wezenlijke wijziging.

4.2.3 [Processor] De Privacy Lead / PIMS Manager MOET informatie ter ondersteuning van monitoringprivacyverklaringen in REG08 verstrekken wanneer de organisatie monitoringdiensten uitvoert op basis van klantinstructies.

4.2.4 [Conditional] De Process Owner / Business Owner MOET alternatieve transparantiemaatregelen in REG07 en REG04 vastleggen voordat niet-zichtbare of noodmonitoring wordt geactiveerd.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Uitzonderingen

9.1 [All] De Privacy Lead / PIMS Manager MOET elke uitzondering op dit beleid in REG12 vastleggen voordat de uitzondering wordt gebruikt.

9.2 [Conditional] De Data Protection Officer / Privacy Advisor MOET privacyadvies in REG04 of REG12 documenteren vóór goedkeuring van uitzonderingen waarbij sprake is van niet-zichtbare monitoring, audio-opname, biometrische identificatie, monitoring met analytics of gevoelige monitoringlocaties.

9.3 [All] Top Management MOET uitzonderingen die langer dan 90 dagen duren in REG12 goedkeuren vóór verlenging na de initiële uitzonderingsperiode.

9.4 [All] De Privacy Lead / PIMS Manager MOET openstaande monitoringuitzonderingen ten minste maandelijks in REG12 beoordelen totdat deze zijn afgesloten.

10. Handhaving

10.1 [All] De Privacy Lead / PIMS Manager MOET falende monitoringbeheersmaatregelen binnen vijf werkdagen na bevestiging als non-conformiteiten in REG12 vastleggen.

10.2 [Both] De Information Security Lead MOET ongeautoriseerde toegang tot monitoringsystemen binnen één werkdag na bevestiging opschorten en de maatregel in REG10 of REG12 vastleggen.

10.3 [All] Top Management MOET binnen 10 werkdagen eigenaarschap voor corrigerende maatregelen in REG12 toewijzen voor herhaalde of wezenlijke beleidsovertredingen.

10.4 [Conditional] De Incident Response Coordinator MOET de workflow voor PII-incidenten in REG10 starten bij vermoedelijke ongeautoriseerde verstrekking, verlies of compromittering van PII uit monitoring.

11. Beoordeling en onderhoud

11.1 [All] De Privacy Lead / PIMS Manager MOET dit beleid en het bijbehorende monitoringbewijsmateriaal ten minste jaarlijks in REG12 beoordelen.

11.2 [Controller] De Process Owner / Business Owner MOET elk actief monitoringdoel, elke privacyverklaring, elke locatiereikwijdte en elke bewaarregistratie in REG02 en REG07 ten minste jaarlijks herbevestigen.

11.3 [Both] De System Owner / Application Owner MOET toegang tot monitoringsystemen, logging, verwijdering en exportbeheersmaatregelen in REG12 ten minste jaarlijks en na een wezenlijke systeemwijziging herbevestigen.

11.4 [Conditional] De Vendor / Procurement Owner MOET bewijsmateriaal voor uitbestede monitoringaanbieders in REG08 ten minste jaarlijks en vóór contractverlenging herbevestigen.

11.5 [All] De Privacy Lead / PIMS Manager MOET gerelateerd bewijsmateriaal in REG02, REG04, REG07, REG08, REG10 of REG12 binnen 30 kalenderdagen na goedgekeurde beleidswijzigingen bijwerken.

12. Gerelateerde beleidslijnen

12.1 PII02 - Beleid inzake privacyrollen, verantwoordelijkheden en verantwoordingsplicht

12.2 PII03 - Beleid inzake inventaris van PII-verwerking en rechtsgrondslag

12.3 PII04 - Beleid inzake privacyverklaringen en transparantie

12.4 PII06 - Beleid inzake beheer van rechten van betrokkenen

12.5 PII07 - Beleid inzake privacyrisicobeoordeling en DPIA

12.6 PII08 - Beleid inzake privacy by design en by default

12.7 PII09 - Beleid inzake verzameling, gebruik, verstrekking en delen van PII

12.8 PII10 - Beleid inzake bewaring, verwijdering en vernietiging van PII

12.9 PII12 - Beleid inzake privacybeheer van verwerkers, subverwerkers en derde partijen

12.10 PII13 - Beleid inzake internationale doorgifte van PII

12.11 PII14 - Beleid inzake PII-beveiliging en toegangscontrole

12.12 PII15 - Beleid inzake incident- en inbreukbeheer voor PII

12.13 PII17 - Beleid inzake gedocumenteerde informatie en bewijsmateriaalbeheer binnen PIMS

12.14 PII18 - Beleid inzake PIMS-monitoring, audit en verbetering

12.15 PII19 - Beleid inzake privacy van werknemers

12.16 PII21 - Privacybeleid voor AI en geautomatiseerde besluitvorming

12.17 PII23 - Beleid voor cloud-PII-verwerkers

13. Referentienormen en -raamwerken

13.1 Dit beleid is gekoppeld aan de volgende normen en regelgeving. De mapping licht toe hoe het beleid de genoemde vereisten ondersteunt en identificeert de interne clausules die deze implementeren of ondersteunen.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Gekoppeld aan gedocumenteerd monitoringbewijsmateriaal, operationele planning, activeringsbeheersmaatregelen, doelregistraties, koppeling aan privacyverklaringen, toegangsconfiguratie, bewaarconfiguratie en wijzigingsbeheer voor CCTV- en fysieke monitoringactiviteiten. Addressed by clauses [4.1.1; 4.1.2; 4.2.2; 4.3.1; 4.4.1; 6.2; 7.1; 11.5].

13.2.2 **Clause 9.1; Clause 10.2** - Gekoppeld aan meting van monitoringbeheersmaatregelen, beoordeling van aanbieders, toegangsbeoordeling, auditbevindingen, non-conformiteiten, corrigerende maatregelen, escalatie van achterstallige acties en verbeterbewijsmateriaal. Addressed by clauses [4.6.4; 6.4; 6.5; 6.6; 8.1; 8.7; 10.1; 11.1].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9** - Gekoppeld aan definitie van monitoringdoelen door de verwerkingsverantwoordelijke, documentatie van de rechtsgrondslag, beslissingen over privacyrisicotriggercriteria en registraties van monitoringverwerkingsactiviteiten in REG02 en REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.4.1; 6.2; 7.1; 11.2].

13.2.4 **Annex A.1.2.7; Annex A.1.2.8** - Gekoppeld aan toewijzing van uitbestede monitoringaanbieders, verdeling van gezamenlijke monitoringverantwoordelijkheden en bewijsmateriaal inzake verwerkers of gezamenlijke verwerkingsverantwoordelijken in REG08. Addressed by clauses [4.1.5; 4.6.1; 4.6.2; 5.7; 6.2; 7.6].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10** - Gekoppeld aan monitoringgerelateerde verplichtingen jegens betrokkenen, routing van verzoeken, bewaring die nodig is om verzoeken te beoordelen en governancebewijsmateriaal voor ondersteuning van rechten. Addressed by clauses [4.5.1; 4.5.2; 5.2; 7.2; 11.5].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Gekoppeld aan beperking van monitoringverzameling, verwerkingsgrenzen, minimalisatie, bewaartermijnen, verwijdering, overschrijving, opschorting van verwijdering en beheersing van uitgenomen kopieën. Addressed by clauses [4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 7.3; 7.5; 8.4].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5** - Gekoppeld aan registraties van externe verstrekking, behandeling van verzoeken om verstrekking, minimalisatie vóór verstrekking en incidentgerelateerde verstrekkingen waarbij PII uit monitoring betrokken is. Addressed by clauses [4.3.4; 4.5.4; 7.8; 10.4].

13.2.8 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Gekoppeld aan klantinstructies voor verwerkers, toegestane verwerkingsgrenzen, ondersteuning voor privacyverklaringen, instructies voor bewaring en verwijdering, bijstand bij rechtenverzoeken en verwerkersregistraties voor uitbestede monitoringdiensten. Addressed by clauses [4.1.6; 4.2.3; 4.4.5; 4.5.3; 4.6.3].

13.2.9 **Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Gekoppeld aan ondersteuning door de verwerker voor klantverplichtingen, autorisatie voor verstrekking, verstrekkingsregistraties, kennisgeving van verzoeken om verstrekking en behandeling van wettelijk bindende verstrekkingen van PII uit monitoring. Addressed by clauses [4.3.5; 4.5.3; 4.6.2; 4.6.3].

13.2.10 **Annex A.3.14; Annex A.3.25** - Gekoppeld aan bescherming van monitoringregistraties, beperkte toegang, beoordeling van geprivilegieerde toegang, toegangslogging, indamming van ongeautoriseerde toegang en loggingbewijsmateriaal voor monitoringsystemen. Addressed by clauses [4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Gekoppeld aan rechtmatigheid, behoorlijkheid, transparantie, doelbinding, gegevensminimalisatie, opslagbeperking en bewijsmateriaal voor verantwoordingsplicht inzake monitoringactiviteiten. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.1; 4.4.2; 4.4.3; 6.1; 8.1; 11.2].

13.3.2 Article 6 - Gekoppeld aan documentatie van de rechtsgrondslag voor CCTV, bezoekersmonitoring, fysieke toegangslogboeken en andere fysieke monitoringactiviteiten. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Gekoppeld aan transparante monitoringprivacyverklaringen, bewijsmateriaal voor bebording, koppeling van privacyverklaringen aan verwerkingsdoelen, informatie van verwerkers ter ondersteuning van privacyverklaringen en alternatieve transparantiemaatregelen. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.2; 8.2; 11.2].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21** - Gekoppeld aan toegang, rectificatie, wissing, beperking, bezwaar, routing van verzoeken, bewaring die nodig is om verzoeken te beoordelen en monitoringgerelateerde klantondersteuning. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.8; 11.5].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Gekoppeld aan governance door de verwerkingsverantwoordelijke, toewijzing van gezamenlijke verwerkingsverantwoordelijken, verwerkersgovernance, verwerkingsregistraties, beveiliging van monitoringsystemen, beoordeling van privacyrisico's, DPIA-triggers en privacyadvies. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 4.3.2; 4.3.3; 4.5.4; 4.6.1; 4.6.2; 4.6.4; 5.1; 5.3; 6.3; 8.5; 10.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Gekoppeld aan doelspecificatie, beperking van gegevensverzameling, gegevensminimalisatie, gebruiksbeperking, bewaarbeperking en verstrekkingsbeperking voor PII uit monitoring. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.4; 4.4.1; 4.4.2; 4.4.4; 7.8].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Gekoppeld aan transparantie, individuele participatie, verantwoordingsplicht, informatiebeveiliging, nalevingsbeoordeling, toegangsbeoordeling, routing van rechtenverzoeken, escalatie van incidenten en bewijsmateriaal voor corrigerende maatregelen. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.1; 4.5.4; 6.1; 8.7; 10.1].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 5.1; Clause 6.2** - Gekoppeld aan privacyrisico en screening op DPIA-triggers voor systematische, niet-zichtbare, audio-, biometrische, door analytics ondersteunde, gevoelige-locatie-, kwetsbare-personen- of andere fysieke monitoring met een hoger risico. Addressed by clauses [4.1.4; 4.2.4; 5.3; 6.3; 7.5; 9.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Gekoppeld aan beheersmaatregelen voor bescherming van PII voor doel, verzameling, minimalisatie, bewaring, verstrekking en participatie van betrokkenen in monitoringcontexten. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.3; 4.5.1; 7.2; 8.2].

13.6.2 **Clause 9.2.3; Clause 9.4.2; Clause 11.1.3** - Gekoppeld aan toegangsverlening, beperking van toegang tot informatie en fysieke toegangsbeheersmaatregelen die relevant zijn voor toegang tot monitoringsystemen en registraties van fysieke toegangscontrole. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 - Gekoppeld aan privacy en bescherming van PII, fysieke toegang, fysieke beveiligingsmonitoring, geprivilegieerde toegang, beperking van toegang tot informatie en loggingbeheersmaatregelen voor CCTV- en fysieke monitoringsystemen. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.3; 7.4; 8.3; 10.2; 11.3].